

01807.001737.

**PATENT APPLICATION**



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**Re Application of:**

PHILIPPE PIRET

Application No.: 09/964,657

Filed: September 28, 2001

For: TURBOCODING METHODS  
WITH A LARGE MINIMUM  
DISTANCE, AND SYSTEMS  
FOR IMPLEMENTING THEM

**Examiner: S. Baker**

Group Art Unit: 2133

November 18, 2004

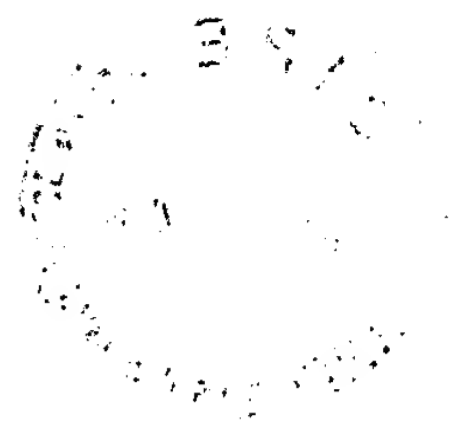
Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

## SUBMISSION OF PRIORITY DOCUMENT

Sir:

In support of Applicant's claim for priority under 35 U.S.C. § 119, enclosed is a certified copy of the following French application:


0012939, filed October 10, 2000.



**THIS PAGE BLANK (USPTO)**

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our address given below.

Respectfully submitted,



---

Raymond A. DiPerna  
Attorney for Applicant  
Registration No. 44,063

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3800  
Facsimile: (212) 218-2200

NY\_MAIN 437037v1

**THIS PAGE BLANK (USPTO)**



A. N. 09/964,657  
GAU 2133

# BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 12 SEP. 2001

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

Martine PLANCHE

**CERTIFIED COPY OF  
PRIORITY DOCUMENT**

**BEST AVAILABLE COPY**

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint Petersburg  
75800 PARIS cedex 08  
Téléphone : 33 (1) 53 04 53 04  
Télécopie : 33 (1) 42 93 59 30  
www.inpi.fr

**THIS PAGE BLANK (USPTO)**

2025 RELEASE UNDER E.O. 14176

<p>REMISE DES PIÈCES</p> <p>DATE <b>10 OCT 2000</b></p> <p>LIEU <b>75 INPI PARIS</b></p> <p>N° D'ENREGISTREMENT <b>0012939</b></p> <p>NATIONAL ATTRIBUÉ PAR L'INPI</p> <p>DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI <b>10 OCT. 2000</b></p>		<p><b>1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE</b> À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE</p> <p>RINUY, SANTARELLI 14, avenue de la Grande Armée 75017 PARIS</p>	
<p><b>Vos références pour ce dossier</b> (facultatif) <b>BIF022422/FR</b></p>			
<p><b>Confirmation d'un dépôt par télécopie</b></p>		<p><input type="checkbox"/> N° attribué par l'INPI à la télécopie</p>	
<p><b>2 NATURE DE LA DEMANDE</b></p> <p>Demande de brevet <input checked="" type="checkbox"/></p> <p>Demande de certificat d'utilité <input type="checkbox"/></p> <p>Demande divisionnaire <input type="checkbox"/></p> <p style="padding-left: 40px;"><i>Demande de brevet initiale</i> N° _____ Date ____/____/____</p> <p style="padding-left: 40px;"><i>ou demande de certificat d'utilité initiale</i> N° _____ Date ____/____/____</p> <p>Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i> <input type="checkbox"/></p> <p style="padding-left: 40px;">N° _____ Date ____/____/____</p>		<p><b>Cochez l'une des 4 cases suivantes</b></p>	
<p><b>3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)</b></p> <p>Procédés de turbocodage circulaire de grande distance minimale, et systèmes pour leur mise en œuvre.</p>			
<p><b>4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE</b></p>		<p>Pays ou organisation _____ N° _____</p> <p>Date ____/____/____</p> <p>Pays ou organisation _____ N° _____</p> <p>Date ____/____/____</p> <p>Pays ou organisation _____ N° _____</p> <p>Date ____/____/____</p> <p><input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»</p>	
<p><b>5 DEMANDEUR</b></p> <p>Nom ou dénomination sociale</p> <p>Prénoms</p> <p>Forme juridique</p> <p>N° SIREN</p> <p>Code APE-NAF</p> <p>Adresse   Rue</p> <p style="padding-left: 40px;">Code postal et ville</p> <p>Pays</p> <p>Nationalité</p> <p>N° de téléphone (facultatif)</p> <p>N° de télécopie (facultatif)</p> <p>Adresse électronique (facultatif)</p>		<p><input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»</p> <p>CANON KABUSHIKI KAISHA</p> <p>Société de droit Japonais</p> <p>30-2, Shimomaruko 3-chome, Ohta-ku</p> <p>Tokyo</p> <p>JAPON</p> <p>JAPONAISE</p>	

REMISE DES PIÈCES DATE <b>10 OCT 2000</b> LIEU <b>75 INPI PARIS</b> N° D'ENREGISTREMENT <b>0012939</b> NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	DB 540 W / 190600
<b>Vos références pour ce dossier :</b> <i>(facultatif)</i>		<b>BIF022422/FR</b>	
<b>6 MANDATAIRE</b> Nom Prénom Cabinet ou Société		<b>RINUY, SANTARELLI</b>	
N° de pouvoir permanent et/ou de lien contractuel			
Adresse	Rue Code postal et ville	<b>14 AVENUE DE LA GRANDE ARMÉE</b> <b>750017 PARIS</b>	
N° de téléphone <i>(facultatif)</i>		<b>01 40 55 43 43</b>	
N° de télécopie <i>(facultatif)</i>			
Adresse électronique <i>(facultatif)</i>			
<b>7 INVENTEUR (S)</b>			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non <b>Dans ce cas fournir une désignation d'inventeur(s) séparée</b>	
<b>8 RAPPORT DE RECHERCHE</b>		<b>Uniquement pour une demande de brevet (y compris division et transformation)</b>	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		<b>Paiement en deux versements, uniquement pour les personnes physiques</b> <input type="checkbox"/> Oui <input type="checkbox"/> Non	
<b>9 RÉDUCTION DU TAUX DES REDEVANCES</b>		<b>Uniquement pour les personnes physiques</b> <input type="checkbox"/> Requête pour la première fois pour cette invention <i>(joindre un avis de non-imposition)</i> <input type="checkbox"/> Requête antérieurement à ce dépôt <i>(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :</i>	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
<b>10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE</b> (Nom et qualité du signataire)		<b>VISA DE LA PRÉFECTURE OU DE L'INPI</b>	
Bruno QUANTIN N° 12.1206 RINUY, SANTARELLI		<b>M. MARTIN</b>	

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

**DÉSIGNATION D'INVENTEUR(S)** Page N° 1. / 1.  
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

<b>Vos références pour ce dossier</b> (facultatif)		BIF022422/FR	
<b>N° D'ENREGISTREMENT NATIONAL</b>		00 12939	
<b>TITRE DE L'INVENTION</b> (200 caractères ou espaces maximum)			
Procédés de turbocodage circulaire de grande distance minimale, et systèmes pour leur mise en oeuvre.			
<b>LE(S) DEMANDEUR(S) :</b>  CANON KABUSHIKI KAISHA			
<b>DESIGNE(NT) EN TANT QU'INVENTEUR(S) :</b> (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
<b>Nom</b>		PIRET	
<b>Prénoms</b>		Philippe	
<b>Adresse</b>	<b>Rue</b>	4, Boulevard des Métairies	
	<b>Code postal et ville</b>	35510	CESSON-SEVIGNE, FRANCE
<b>Société d'appartenance (facultatif)</b>			
<b>Nom</b>			
<b>Prénoms</b>			
<b>Adresse</b>	<b>Rue</b>		
	<b>Code postal et ville</b>		
<b>Société d'appartenance (facultatif)</b>			
<b>Nom</b>			
<b>Prénoms</b>			
<b>Adresse</b>	<b>Rue</b>		
	<b>Code postal et ville</b>		
<b>Société d'appartenance (facultatif)</b>			
<b>DATE ET SIGNATURE(S)</b> <b>DU (DES) DEMANDEUR(S)</b> <b>OU DU MANDATAIRE</b> (Nom et qualité du signataire)		Le 6 octobre 2000 Bruno QUANTIN N° 1206 RINUY, SANTAREL	

**DOCUMENT COMPORTANT DES MODIFICATIONS**

PAGE(S) DE LA DESCRIPTION OU DES REVENDEICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
20a22				8. 11. 2000	23-11. 2000 AL

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifiées).

La présente invention concerne les systèmes de communication dans lesquels, afin d'améliorer la fidélité de la transmission, les données à transmettre sont soumises à un codage de canal. Elle concerne plus particulièrement un procédé de « turbocodage », ainsi que les dispositifs et  
 5 appareils destinés à mettre en œuvre ce procédé.

On rappelle que le codage dit « de canal » consiste, quand on forme les « mots de code » envoyés au récepteur, à introduire une certaine redondance dans les données à transmettre. Au niveau du récepteur, le procédé de décodage associé exploite alors judicieusement cette redondance  
 10 pour détecter d'éventuelles erreurs de transmission et si possible les corriger. Plus précisément, on définit la « distance de Hamming » entre deux séquences binaires de même longueur comme étant le nombre d'emplacements où les deux séquences possèdent un élément binaire différent. Les mots de code obéissent à certaines règles définies par le procédé de codage considéré, ce  
 15 qui permet au récepteur de remplacer le mot reçu par le mot de code « légal » situé à la distance de Hamming la plus courte de ce mot reçu.

Il est clair que cette procédure de correction d'erreurs est d'autant plus fiable que la distance de Hamming minimale entre les divers mots de code est plus grande. On notera que la distance entre un mot de code donné et le  
 20 mot de code « nul » (celui dont tous les éléments binaires sont nuls) est égale au nombre d'éléments binaires égaux à 1, appelé « poids binaire », de ce mot de code donné. On en déduit qu'un procédé de codage est, toutes choses égales par ailleurs, d'autant meilleur que la « distance minimale » du code, c'est-à-dire, la valeur minimale du poids binaire de ses mots de code (à  
 25 l'exclusion du mot nul) est élevée. Pour plus de détails, on se référera par exemple au livre « Computer Networks » de A. Tannenbaum, 3<sup>ème</sup> édition, Prentice-Hall International, New Jersey, 1996, page 184.

On connaît en particulier les procédés de codage appelés « codes cycliques redondants ». Dans chacun d'eux, on a fait le choix d'un polynôme  
 30  $g(x)$ , dit « polynôme générateur », à coefficients binaires, de degré  $d$  et de terme constant égal à 1. On met chaque séquence d'informations à transmettre, éventuellement en la prolongeant avec des éléments nuls, sous la

forme d'une séquence binaire  $\underline{u}$  ayant une longueur  $k$  fixe. Puis on forme une séquence  $\underline{a}$  en prolongeant la séquence  $\underline{u}$  au moyen d'un nombre de bits égal à  $d$ , ces bits dits de « bourrage » (« *padding bits* » en anglais) étant choisis de manière à ce que le polynôme

$$5 \quad a(x) = \sum_{i=0}^{k+d-1} a_i x^i$$

associé à  $\underline{a}$  soit divisible par  $g(x)$  (modulo 2). Ce sont les séquences  $\underline{a}$  (de longueur  $p = k + d$ ) qui sont envoyées au récepteur. Les erreurs de transmission sont alors détectées en examinant le reste de la division du mot de code reçu par le polynôme générateur (voir par exemple A. Tannenbaum, 10 *op. cit.*, pages 187-188).

On a proposé récemment des procédés de codage très efficaces, appelés « turbocodes », dans lesquels on accroît la redondance en transmettant, pour chaque séquence  $\underline{u}$  de données initiales, non pas une seule, mais trois séquences binaires  $\underline{a}$ ,  $\underline{b}$  et  $\underline{c}$ , obtenues comme expliqué ci-après. Les 15 turbocodes font partie des codes dits « convolutifs », c'est-à-dire des codes dans lesquels chaque bit entrant dans un codeur est combiné à d'autres bits provisoirement enregistrés dans ce codeur, ces bits provisoirement enregistrés ayant été produits par le traitement, dans le codeur, des bits entrants précédents ; de ce fait, le résultat du codage d'une séquence entrant dans un 20 codeur convolutif dépend en général des séquences traitées précédemment.

La séquence  $\underline{b}$  que l'on vient de mentionner est obtenue à l'aide d'un dispositif que nous appellerons le « premier codeur », habituellement sur la base de la représentation polynomiale

$$b(x) = a(x) \cdot f_1(x) / g(x),$$

25 où  $a(x)$  est le polynôme associé à ladite séquence  $\underline{a}$ ,  $g(x)$  un premier polynôme prédéterminé à coefficients binaires de degré  $d$  et de terme constant égal à 1, et  $f_1(x)$  un deuxième polynôme prédéterminé à coefficients binaires sans diviseur commun avec  $g(x)$ . Le polynôme  $g(x)$  est appelé « polynôme de récurrence » en raison de son apparition au dénominateur de l'expression ci- 30 dessus.

Quant à la séquence  $\underline{a}$ , elle peut être prise identique à  $\underline{u}$ , mais elle est souvent obtenue, comme dans les « codes cycliques redondants », en prolongeant la séquence  $\underline{u}$  au moyen de bits de bourrage choisis de manière à ce que  $a(x)$  soit divisible par  $g(x)$ . En effet, comme il est connu de l'homme du  
 5 métier, cette divisibilité est une condition nécessaire pour garantir la même qualité de décodage pour les derniers bits de chaque séquence que pour les autres bits.

La séquence  $\underline{c}$ , enfin, est obtenue à l'aide d'un dispositif que nous appellerons le « second codeur », habituellement sur la base de la  
 10 représentation polynomiale

$$c(x) = a^*(x) \cdot f_2(x) / g^*(x),$$

où  $g^*(x)$  est un troisième polynôme prédéterminé à coefficients binaires de degré  $d$  et de terme constant égal à 1, où  $f_2(x)$  est un quatrième polynôme prédéterminé à coefficients binaires, sans diviseur commun avec  $g^*(x)$ , et où le  
 15 polynôme  $a^*(x)$  représente une séquence binaire  $\underline{a}^*$  qui résulte de manière prédéterminée d'une permutation des éléments binaires de  $\underline{u}$  ou de  $\underline{a}$  (opération appelée « entrelaçage »).

Le « turbodécodage » du message transmis fonctionne de la manière suivante : le décodeur reçoit trois séquences de nombres, notées  $\underline{a}'$ ,  $\underline{b}'$   
 20 et  $\underline{c}'$ , et qui ont été produites par l'action du bruit du canal de transmission sur les séquences émises  $\underline{a}$ ,  $\underline{b}$  et  $\underline{c}$ . Le turbodécodeur met alors en œuvre un processus itératif (utilisant  $\underline{b}'$  et  $\underline{c}'$  en alternance) destiné à calculer une valeur estimée  $\hat{\underline{a}}$  de  $\underline{a}$  avec une fiabilité qui croît avec le nombre d'itérations choisi. Si  
 25 l'on a utilisé des bits de bourrage, il suffit évidemment, une fois la valeur finale de  $\hat{\underline{a}}$  obtenue, d'en supprimer les  $d$  derniers bits pour obtenir la valeur estimée  $\hat{\underline{u}}$  de  $\underline{u}$ .

Les remarques faites ci-dessus concernant l'utilité de la divisibilité des polynômes  $a(x)$  par le polynôme  $g(x)$  au niveau du premier codeur s'appliquent également au niveau du second codeur, pour lequel se pose le  
 30 problème de la divisibilité des polynômes  $a^*(x)$  par le polynôme de récurrence  $g^*(x)$ , ce problème devant être résolu dans le cadre où chacun de ces polynômes  $a^*(x)$  est issu d'un polynôme  $a(x)$  divisible par  $g(x)$ . Une solution

connue consiste, en premier lieu, à permuter de manière prédéterminée les éléments binaires de  $\underline{u}$  pour obtenir une séquence  $\underline{u}^*$ , et, en second lieu, à former  $\underline{a}^*$  en prolongeant  $\underline{u}^*$  au moyen de  $d$  bits de bourrage de manière à ce que  $\underline{a}^*(x)$  soit divisible par  $g^*(x)$  (on choisira alors de préférence  $g^*(x)$  identique à  $g(x)$  par souci de simplicité) ; mais un tel procédé de turbocodage présente l'inconvénient que l'efficacité du turbodécodage n'est pas idéale en raison du fait que  $\underline{a}$  et  $\underline{a}^*$  contiennent des jeux de bits de bourrage choisis indépendamment l'un de l'autre ; il en résulte une certaine perte de fiabilité (mesurée en termes de taux d'erreurs) de la transmission.

10 La demande de brevet EP 0 928 071, au nom de CANON, résout ce problème délicat grâce à des entrelaceurs dans lesquels la séquence  $\underline{a}^*$  est obtenue directement par permutation des éléments binaires de  $\underline{a}$ . Plus précisément, on représente  $\underline{a}^*$  par le polynôme

$$a^*(x) = \sum_{i=0}^{p-1} a_i x^{\pi(i)},$$

15 où  $\pi(i)$  appartient à une certaine classe de permutations des entiers  $i$  compris entre 0 et  $(p-1)$  ; pour chacun de ces entrelaceurs, on peut toujours trouver un polynôme  $g^*(x)$  tel que, quel que soit le polynôme  $a(x)$  divisible par  $g(x)$ , le polynôme  $a^*(x)$  soit également divisible par  $g^*(x)$ . Ainsi, une fois la séquence  $\underline{a}$  constituée, on n'a pas à ajouter de bits de bourrage supplémentaires pour  
20 obtenir  $\underline{a}^*$ .

Outre une distance minimale élevée, une deuxième qualité recherchée pour un procédé de codage est évidemment sa simplicité de mise en œuvre, c'est à dire la simplicité de l'algorithme employé, tant au niveau du codage que du décodage associé.

25 A cet effet, le document EP 0 928 071 mentionné ci-dessus présente un exemple particulier de permutation appartenant à ladite classe des permutations préservant la divisibilité : on y prend pour  $\pi(i)$  le résidu modulo  $p$  du produit  $(i \cdot e)$ , où  $e$  est un nombre entier strictement positif prédéterminé, relativement premier avec  $p$  et congru à une puissance de 2 modulo  $p$  ; il en  
30 résulte que  $g^*(x)$  est simplement égal à  $g(x)$ .

Cet entrelaceur, qui a le mérite de la simplicité, présente toutefois l'inconvénient de requérir que la longueur  $p$  des séquences  $\underline{a}$  et  $\underline{a}^*$  soit un multiple impair de la période du polynôme de récurrence (la période d'un polynôme  $g(x)$  est définie comme étant le plus petit entier positif  $N$  tel que ledit polynôme  $g(x)$  divise  $(x^N + 1)$  modulo 2 ; pour d'autres propriétés déjà connues de ladite période, on pourra consulter l'ouvrage classique de F.J. Mc Williams et N.J.A. Sloane intitulé « *The Theory of Error-Correcting Codes* », publié par North-Holland en 1977 et dont la septième édition a eu lieu en 1992).

Afin de permettre un plus grand choix dans la longueur desdites séquences tout en préservant les avantages offerts par les entrelaceurs selon EP 0 928 071, l'invention propose un procédé de tubocodage pour la transmission d'informations dans lequel, un premier polynôme à coefficients binaires  $g(x)$  de degré  $d$  et de terme constant égal à 1 ayant été prédéterminé, on présente d'abord lesdites informations sous la forme de séquences binaires  $\underline{u}$  de longueur

$$k = p - d,$$

où  $p$  est un multiple prédéterminé de la période  $N$  dudit polynôme  $g(x)$ , puis l'on produit pour chacune desdites séquences  $\underline{u}$  un triplet  $\underline{v}$  de séquences binaires  $(\underline{a}, \underline{b}, \underline{c})$  destinées à être transmises et obtenues comme suit :

- ladite séquence  $\underline{a}$  est de longueur  $p$  et obtenue en prolongeant la séquence  $\underline{u}$  au moyen de  $d$  bits de « bourrage » de manière à ce que le polynôme

$$a(x) = \sum_{i=0}^{p-1} a_i x^i$$

associé à  $\underline{a}$  soit divisible par  $g(x)$ ,

- ladite séquence  $\underline{b}$  est représentée par le polynôme

$$b(x) = a(x) \cdot f_1(x) / g(x),$$

où  $f_1(x)$  est un deuxième polynôme à coefficients binaires prédéterminé, sans diviseur commun avec  $g(x)$ , et

- ladite séquence  $\underline{c}$  est représentée par le polynôme

$$c(x) = a^*(x) \cdot f_2(x) / g^*(x),$$

où

$$a^*(x) = \sum_{i=0}^{p-1} a_i x^{\pi(i)},$$

où  $\pi(i)$  est une permutation prédéterminée des entiers  $i$  compris entre 0 et  $(p-1)$ , où  $g^*(x)$  est un troisième polynôme à coefficients binaires prédéterminé, de degré  $d$  et de terme constant égal à 1,  $\pi(i)$  et  $g^*(x)$  étant choisis de manière  
 5 à ce que, quel que soit le polynôme  $a(x)$  divisible par  $g(x)$ ,  $a^*(x)$  soit divisible par  $g^*(x)$ , et où  $f_2(x)$  est un quatrième polynôme à coefficients binaires prédéterminé, sans diviseur commun avec  $g^*(x)$ , caractérisé en ce que l'on prend pour  $\pi(i)$  le résidu modulo  $p$  du produit  $(i \cdot e)$ , où  $e$  est un nombre entier strictement positif prédéterminé, relativement premier  
 10 avec  $p$ , congru à une puissance de 2 modulo  $N$ , et non congru à une puissance de 2 modulo  $p$ , d'où il résulte que  $g^*(x)$  est identique à  $g(x)$ .

Corrélativement, l'invention concerne un procédé de turbodécodage, ledit procédé étant remarquable en ce qu'il permet de décoder des séquences reçues qui ont été émises après avoir été codées à l'aide d'un procédé de  
 15 turbocodage selon l'invention.

Ainsi, les procédés de turbocodage selon l'invention, bien que ne requérant pas de bits de bourrage supplémentaires pour obtenir la séquence « entrelacée »  $\underline{a}^*$ , sont applicables à une large gamme de longueurs  $p$  de séquences émises (puisque  $M=p/N$  peut être pair ou impair), tout en restant  
 20 relativement simples à mettre en œuvre.

De plus, les procédés de turbocodage selon la présente invention, tout en s'inscrivant dans le cadre général des permutations divulguées par EP 0 928 071, permettent à l'homme du métier d'accéder, dans le cas où il choisit  $M$  impair, à un plus grand réservoir de valeurs du nombre  $e$  parmi lesquelles il  
 25 pourra choisir une valeur optimale  $e^*$ , par comparaison avec l'exemple particulier de permutation divulgué par EP 0 928 071 et mentionné ci-dessus.

En effet, cet exemple particulier de permutation offre déjà un ensemble assez large de valeurs possibles pour  $e$ , défini (entre autres critères) par le fait que chaque nombre  $e$  dans cet ensemble est congru à une  
 30 puissance de 2 modulo  $p$ . Or des recherches ultérieures ont permis à l'inventeur d'accéder à un réservoir supplémentaire de valeurs de  $e$  définissant,

ici encore, des permutations préservant la divisibilité : il s'agit (entre autres critères) des entiers congrus à une puissance de 2 modulo  $N$  qui ne sont pas congrus à une puissance de 2 modulo  $p$ . Non seulement les nouvelles valeurs de  $e$  ainsi mises en évidence permettent une mise en œuvre pratique d'un  
 5 turbocodage avec les mêmes avantages qu'un turbocodage selon l'exemple divulgué par EP 0 928 071, mais en outre l'homme du métier pourra, en fonction des conditions concrètes de mise en œuvre, rechercher ladite valeur optimale  $e^*$  à la fois dans les valeurs de l'ensemble connu et dans les valeurs du réservoir supplémentaire fourni par la présente invention.

10 Il est notamment souhaitable d'utiliser un code de grande distance minimale (comme on l'a expliqué en introduction, la distance minimale du code joue un rôle important dans l'aptitude du code à détecter et corriger les erreurs de transmission). Dans ce but, on procédera de la manière suivante pour déterminer une valeur optimale  $e^*$  de  $e$  :

15 a) on choisit un certain nombre de séquences  $\underline{u}$  différentes pour former ce que l'on appellera « l'ensemble représentatif »,

b) pour chaque nombre entier strictement positif  $e$  inférieur à  $p$ , congru à une puissance de 2 modulo  $N$  et relativement premier avec  $p$  :

- on calcule le poids binaire  $PB$  total de tous lesdits triplets de  
 20 séquences binaires  $\underline{v}$  associés aux séquences  $\underline{u}$  appartenant audit ensemble représentatif, et

- on prend note de la valeur  $w(e)$ , associée à cette valeur de  $e$ , du poids minimal parmi tous ces poids binaires  $PB$ , et

c) on choisit, pour mettre en œuvre le codage, la valeur  $e^*$  de  $e$  qui  
 25 est associée à la plus grande valeur de ce poids minimal  $w$ .

Grâce à ces dispositions, les codes selon l'invention bénéficient d'un poids minimal relativement élevé, quels que soient lesdits polynômes prédéterminés choisis.

Selon un autre de ses aspects, l'invention concerne divers  
 30 dispositifs.

Elle concerne ainsi un dispositif de codage de séquences de données destinées à être transmises à l'aide d'un procédé de turbocodage selon l'invention, ledit dispositif étant remarquable en ce qu'il comporte :

- des moyens pour obtenir, pour chaque séquence de données  $\underline{u}$ , ladite
- 5 séquence  $\underline{a}$  associée à  $\underline{u}$  en prolongeant la séquence  $\underline{u}$  au moyen desdits  $d$  bits de bourrage, et
- au moins un turbocodeur comportant un entrelaceur  $\pi_1$  apte à réaliser la permutation prévue dans ledit procédé.

Corrélativement, l'invention concerne un dispositif de décodage

10 destiné à mettre en œuvre un procédé de turbodécodage selon l'invention, ledit dispositif étant remarquable en ce qu'il comporte :

- au moins un turbodécodeur comportant deux entrelaceurs  $\pi_1$  aptes à réaliser la permutation prévue dans ledit procédé, et un désentrelaceur  $\pi_2$  apte à inverser cette permutation, et
- 15 - des moyens pour produire une séquence binaire  $\hat{\underline{u}}$  en ôtant les  $d$  derniers bits de la séquence estimée  $\hat{\underline{a}}$  obtenue à la fin du turbodécodage des séquences reçues  $\underline{a'}$ ,  $\underline{b'}$  et  $\underline{c'}$  correspondant respectivement auxdites séquences émises  $\underline{a}$ ,  $\underline{b}$ , et  $\underline{c}$ .

La présente invention vise également :

- 20 - un appareil d'émission de signaux numériques codés, comportant un dispositif de codage tel que décrit succinctement ci-dessus, et comportant des moyens pour émettre lesdites séquences codées  $\underline{a}$ ,  $\underline{b}$ , et  $\underline{c}$ ,
- un appareil de réception de signaux numériques codés, comportant un dispositif de décodage tel que décrit succinctement ci-dessus, et comportant
- 25 des moyens pour recevoir lesdites séquences  $\underline{a'}$ ,  $\underline{b'}$ , et  $\underline{c'}$ ,
- un réseau de télécommunications, comportant au moins un appareil d'émission ou un appareil de réception de signaux numériques codés tels que décrits succinctement ci-dessus,
- un moyen de stockage de données lisible par un ordinateur ou un
- 30 microprocesseur conservant des instructions d'un programme informatique, permettant la mise en œuvre de l'un des procédés selon l'invention,
- un moyen de stockage de données amovibles, partiellement ou

totale, lisible par un ordinateur et/ou un microprocesseur conservant des instructions d'un programme informatique, permettant la mise en œuvre de l'un des procédés selon l'invention, et

- un programme d'ordinateur, contenant des instructions telles que, lorsque ledit programme commande un dispositif de traitement de données programmable, lesdites instructions font que ledit dispositif de traitement de données met en œuvre l'un des procédés selon l'invention.

Les avantages offerts par ces dispositifs, appareils de traitement de signaux numériques, réseaux de télécommunications, moyens de stockage de données et programmes d'ordinateur sont essentiellement les mêmes que ceux offerts par les procédés selon l'invention.

D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée, que l'on trouvera ci-dessous, d'un mode de réalisation préféré donné à titre d'exemple non limitatif. Cette description se réfère aux dessins annexés, dans lesquels :

- la figure 1 est un organigramme illustrant les étapes successives conduisant à la sélection d'un procédé de codage particulier selon l'invention,
- la figure 2 représente de façon schématique un dispositif de codage selon l'invention,
- la figure 3a représente de façon schématique le fonctionnement classique du premier codeur,
- la figure 3b représente de façon schématique le fonctionnement classique du second codeur,
- la figure 4 représente de façon schématique un appareil d'émission de signaux numériques selon l'invention,
- la figure 5 représente de façon schématique un dispositif de turbodécodage selon l'invention,
- la figure 6 représente de façon schématique un appareil de réception de signaux numériques selon l'invention,
- la figure 7 représente de façon schématique un réseau de télécommunications sans fil susceptible de mettre en œuvre l'invention, et
- la figure 8 est un graphique illustrant les résultats d'une simulation

d'un procédé de codage et décodage selon l'invention.

Pour commencer, on va expliquer, à l'aide d'exemples numériques, les principes mathématiques sur lesquels repose l'invention.

Choisissons par exemple le polynôme

$$5 \quad g(x) = 1 + x + x^3,$$

de degré  $d = 3$ , comme polynôme de récurrence. Il divise  $(x^7+1)$  (le quotient étant  $(1+x+x^2+x^4)$ ), mais ne divise pas  $(x^N + 1)$  pour  $N$  compris entre 1 et 6 : la période de ce polynôme  $g(x)$  est donc égale à 7.

Prenons maintenant par exemple une longueur de séquences  
10 transmises égale à

$$p = 14, \text{ soit : } M = p/N = 2.$$

Pour trouver les valeurs possibles de  $e$ , l'on recherche d'abord les entiers congrus à une puissance de 2 modulo 7 ( $N$  étant égal à 7), c'est-à-dire congrus à 1, 2, ou 4, en se limitant aux valeurs inférieures à 14 ( $p$  étant égal à  
15 14) qui sont les seules valeurs utiles puisque les différentes permutations se distinguent par les résidus de  $(i \cdot e)$  modulo 14 ; les valeurs correspondantes sont : 1, 2, 4, 8, 9, et 11. Enfin, en éliminant les valeurs 2, 4 et 8, qui ont chacune un diviseur commun avec 14 (et qui ne donneraient pas lieu, par conséquent, à une permutation des 14 indices concernés), on trouve que, pour  
20 cet exemple, les valeurs « utiles » de  $e$  sont 1, 9 et 11.

L'exemple que nous venons d'étudier comporte une longueur de séquences qui est un multiple pair de  $N$ , longueur incompatible avec les procédés selon EP 0 928 071. On va montrer à présent, sur la base d'un deuxième exemple, que la présente invention est avantageuse par rapport à  
25 cet art antérieur, même dans le cas où  $M$  est impair. Considérons donc, avec le même  $g(x)$  que ci-dessus, le cas  $p = 63$  (soit :  $M = 9$ ). On trouve aisément que les entiers  $e$  congrus à une puissance de 2 modulo 63 (et donc aussi congrus à une puissance de 2 modulo 7) « utiles » sont :

$$e = 1, 2, 4, 8, 16, 32.$$

30 Or la présente invention permet de choisir  $e$  également parmi les valeurs :

$$e = 11, 22, 23, 25, 29, 37, 43, 44, 46, 50, 53, 58$$

correspondant aux entiers congrus à une puissance de 2 modulo 7, mais non

congrus à une puissance de 2 modulo 63.

Construisons à présent une permutation selon l'invention, par exemple dans le cas, étudié ci-dessus, où  $p = 14$  et  $e = 9$ . En prenant les résidus de  $(9i)$  modulo 14 pour  $i$  compris entre 0 et 13, on trouve facilement :

$$\begin{aligned} 5 \quad a^*_0 = a_0, a^*_1 = a_{11}, a^*_2 = a_8, a^*_3 = a_5, a^*_4 = a_2, a^*_5 = a_{13}, a^*_6 = a_{10}, a^*_7 = a_7, \\ a^*_8 = a_4, a^*_9 = a_1, a^*_{10} = a_{12}, a^*_{11} = a_9, a^*_{12} = a_6, \text{ et } a^*_{13} = a_3. \end{aligned} \quad (1)$$

Examinons l'effet de cette permutation sur une séquence de données quelconque, par exemple :

$$\underline{u} = (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0).$$

10 En prolongeant  $\underline{u}$  avec les 3 ( $d$  étant égal à 3) bits  $(1, 0, 1)$ , on obtient

$$\underline{a} = (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1), \text{ soit}$$

$$a(x) = 1 + x^3 + x^7 + x^{11} + x^{13},$$

qui est bien divisible par  $g(x)$  (le quotient étant égal à  $(1 + x + x^2 + x^3 + x^5 + x^7 + x^{10})$ ). A l'aide de l'équation (1), on obtient alors la séquence  $\underline{a}^*$  représentée par

15 le polynôme

$$a^*(x) = 1 + x + x^5 + x^7 + x^{13},$$

qui est bien divisible par  $g(x)$  (le quotient étant égal à  $(1 + x^3 + x^4 + x^6 + x^7 + x^8 + x^{10})$ ), conformément au but visé par l'invention.

20 On peut montrer que, quelle que soit la permutation selon l'invention, le polynôme  $g^*(x)$  adéquat n'est autre que  $g(x)$ .

On voit ainsi que le choix d'abord de  $g(x)$ , puis de  $p$  conduit, en appliquant les règles ci-dessus, à un ensemble «  $E$  » de valeurs « utiles » de  $e$ . Il ne reste plus alors qu'à choisir les polynômes  $f_1(x)$  et  $f_2(x)$ , et à fixer une valeur de  $e$  qui soit la plus efficace possible en termes de taux d'erreurs  
25 résiduelles après décodage, pour obtenir un procédé de turbocodage particulier conforme à l'invention.

De manière générale, la procédure conduisant à la sélection d'un procédé selon l'invention comprendra de préférence les étapes suivantes, décrites en référence à la **Figure 1**. A l'étape 1201, on choisit un polynôme de  
30 récurrence  $g(x)$  déterminé, ainsi que les polynômes  $f_1(x)$  et  $f_2(x)$ , sur la base de critères bien connus du spécialiste des procédés de codage récursifs (on prend habituellement des polynômes  $f_1(x)$  et  $f_2(x)$  de même degré  $d$  que  $g(x)$ ). A

l'étape 1202, on calcule la période  $N$  du polynôme  $g(x)$ . A l'étape 1203, on choisit la longueur  $p$  des séquences codées  $\underline{a}$  à transmettre ; cette longueur doit, selon l'invention, être un multiple de  $N$  ; le respect des normes techniques associées au canal de transmission concerné limitera aussi, habituellement, les possibilités de choix. A l'étape 1204, on calcule toutes les valeurs « utiles » de  $e$ , c'est-à-dire l'ensemble  $E$  des entiers compris entre 1 et  $p$  qui sont congrus à une puissance de 2 modulo  $N$  et relativement premiers (c'est-à-dire, sans diviseur commun) avec  $p$ . A l'étape 1205, on détermine un ensemble «  $U$  » de séquences binaires  $\underline{u}$ , chacune de longueur  $k = p - d$ , destiné à représenter la totalité des séquences de données possibles ; on peut ici, soit engendrer un tel ensemble d'après des règles préétablies, soit faire appel à une banque de données où un tel ensemble a déjà été enregistré. A l'étape 1206, on calcule, par bourrage (comme expliqué ci-dessus), toutes les séquences  $\underline{a}$  correspondant aux séquences  $\underline{u}$  contenues dans  $U$ , de façon à constituer un ensemble «  $A$  ». A l'étape 1207, on considère tour à tour toutes les valeurs de  $e$  contenues dans  $E$  ; pour chacune d'elles, on calcule d'abord la permutation associée, comme on l'a fait dans l'exemple numérique ci-dessus ; puis l'on calcule, par des multiplications et divisions de polynômes, tous les triplets  $\underline{v}$  correspondant aux éléments de «  $A$  », de façon à constituer un ensemble «  $V$  » ; puis l'on calcule le poids binaire  $PB$  de chaque élément de «  $V$  » ; enfin, l'on détermine le minimum  $w$ , parmi tous ces poids  $PB$ , associé à cette valeur particulière de  $e$ , et l'on enregistre la fonction  $w(e)$ . La valeur de  $e$  optimale pour ce turbocode, c'est-à-dire, associée à la plus grande distance minimale possible, est finalement obtenue, à l'étape 1208, en identifiant la valeur de  $e$  qui fournit la valeur maximale du poids minimal  $w$ .

La **figure 2** représente un dispositif de codage selon l'invention, dans lequel le codage des données aux fins de transmission est effectué par un turbocodeur constitué de deux codeurs convolutifs et d'un entrelaceur  $\pi_1$  (système à deux parités).

On rappelle qu'un turbocodeur classique est constitué de deux codeurs convolutifs récurrents systématiques (en anglais : RSC, « *Recursive Systematic Convolutional* ») et d'un entrelaceur, disposés comme le montre la

figure 2. Le turbocodeur fournit, en sortie, pour chaque séquence d'éléments binaires entrante  $\underline{a}$ , trois séquences d'éléments binaires ( $\underline{a}$ ,  $\underline{b}$ ,  $\underline{c}$ ), où  $\underline{a}$  est la sortie dite « systématique » du turbocodeur, c'est-à-dire n'ayant subi aucune modification par rapport au signal d'entrée,  $\underline{b}$  est la sortie codée par le premier codeur (désigné par RSC1) et  $\underline{c}$  est la sortie codée par le second codeur (désigné par RSC2) après passage dans l'entrelaceur  $\pi_1$ .

Dans le mode préféré de réalisation, le signal transportant la séquence de données  $\underline{u}$  alimente un module de bourrage 30. Ce module 30 est chargé de prolonger la séquence  $\underline{u}$  au moyen de bits de bourrage, comme expliqué ci-dessus, de manière à obtenir une séquence  $\underline{a}$  dont la longueur  $p$  est un multiple de la période  $N$  du polynôme  $g(x)$ , et dont le polynôme associé  $a(x)$  est divisible par  $g(x)$ . Le signal résultant alimente alors le turbocodeur 40. Ce dernier comporte un entrelaceur  $\pi_1$  selon l'invention, c'est-à-dire produisant, à partir de la séquence  $\underline{a}$ , une permutation  $\underline{a}^*$  divisible par  $g(x)$ .

Les procédés selon l'invention ont ainsi pour conséquence que l'état final de chaque codeur (c'est-à-dire à la fin du codage d'une séquence quelconque) est identique à son état initial (au début du codage de ladite séquence), ce qui garantit une qualité de décodage uniforme pour tous les bits d'une même séquence. Lesdits états des codeurs sont représentés sur les figures 3a et 3b.

La **figure 3a** est un schéma de fonctionnement du premier codeur RSC (celui produisant une séquence  $\underline{b}$  à partir d'une séquence  $\underline{a}$ ), dans le cas où l'on prend, par exemple,

$$f_1(x) = 1 + x^2 + x^3, \text{ et}$$

$$g(x) = 1 + x + x^3.$$

Ce codeur porte en mémoire trois bits  $s_1$ ,  $s_2$ , et  $s_3$ .

La **figure 3b** est un schéma de fonctionnement du second codeur RSC (celui produisant une séquence  $\underline{c}$  à partir d'une séquence  $\underline{a}^*$ ), dans le cas où l'on prend, par exemple,

$$f_2(x) = 1 + x + x^2 + x^3, \text{ et}$$

$$g^*(x) = 1 + x + x^3.$$

Ce codeur porte en mémoire trois bits  $s^*_1$ ,  $s^*_2$ , et  $s^*_3$ .

Ces deux codeurs RSC sont illustrés sur les figures 3a et 3b sous la forme d'éléments de retard, tels que des bascules par exemple. Ces séquences d'éléments de retard réalisent les fonctions logiques représentées par des multiplications ou des divisions par des polynômes. Cette  
 5 représentation est classique et bien connue de l'homme du métier.

Enfin, le turbocodeur 40 envoie les trois séquences de données a, b, et c ainsi obtenues vers l'émetteur 906 (voir la figure 4).

Pour plus de détails sur les turbocodes, on se reportera utilement

- à l'article de C. Berrou, A. Glavieux et P. Thitimajshima intitulé « *Near*  
 10 *Shannon Limit Error-Correcting Coding and Decoding: Turbo-codes* », ICC '93, Genève (édité par IEEE, Piscataway, NJ, USA, 1993),

- à l'article de R. de Gaudenzi et M. Luise intitulé « *Audio and Video Digital Radio Broadcasting Systems and Techniques* », Actes du Sixième Séminaire International de Tirrenia sur les Télécommunications Numériques,  
 15 pages 215 à 226 (1993),

- à l'article de J. Hagenauer, P. Robertson et L. Papke intitulé « *Iterative (Turbo) Decoding of Systematic Convolutional Codes with the MAP and SOVA Algorithms* », Informationstechnische Gesellschaft (ITG) Fachbericht, pages 21 à 29 (octobre 1994),

20 - à l'article de J. Hagenauer, E. Offer et L. Papke intitulé « *Iterative Decoding of Binary Block and Convolutional Codes* », IEEE Transactions on Information Theory (édité par IEEE, Piscataway, NJ, USA, 1996),

- à l'article de C. Berrou, S. Evano et G. Battail intitulé « *Turbo-block Codes* », Actes du séminaire « *Turbo-Coding* » organisé par le Département  
 25 d'électronique appliquée de l'Institut de Technologie de Lund, Suède) (août 1996), et

- à l'article de C. Berrou et A. Glavieux intitulé « *Near Optimum Error-Correcting Coding and Decoding: Turbo-Codes* », IEEE Transactions on Communications, vol. 44, n° 10, pages 1261 à 1271 (édité par IEEE,  
 30 Piscataway, NJ, USA, 1996).

La **figure 4** montre, de façon très schématique, un appareil d'émission de signaux numériques 48 selon l'invention. Ce dernier comprend,

un clavier 911, un écran 909, une source d'informations externe 910, un émetteur hertzien 906, conjointement reliés à des ports d'entrée/sortie 903 d'un dispositif de codage 901 qui est réalisé ici sous la forme d'une unité logique.

Le dispositif de codage 901 comporte, reliés entre eux par un bus d'adresses et de données 902 :

- une unité centrale de traitement 900,
- une mémoire vive RAM 904,
- une mémoire morte 905, et
- lesdits ports d'entrée/sortie 903.

Chacun des éléments illustrés en figure 4 est bien connu de l'homme du métier des micro-ordinateurs et des systèmes de transmission et, plus généralement, des systèmes de traitement de l'information. Ces éléments connus ne sont donc pas décrits ici. On observe, cependant, que :

- la source d'informations 910 pourrait être, par exemple, un périphérique d'interface, un capteur, un démodulateur, une mémoire externe ou un autre système de traitement de l'information (non représenté), et pourrait par exemple fournir des séquences de signaux représentatifs de parole, de messages de service ou de données multimédia notamment de type IP ou ATM, sous forme de séquences de données binaires,
- l'émetteur hertzien 906 est adapté à mettre en œuvre un protocole de transmission par paquets sur un canal non filaire, et à transmettre ces paquets sur un tel canal.

La mémoire vive 904 conserve des données, des variables et des résultats intermédiaires de traitement, dans des registres de mémoire portant, dans la description, les mêmes noms que les données dont ils conservent les valeurs. On observera, au passage, que le mot « registre » désigne, à travers la présente description, aussi bien une zone mémoire de faible capacité (quelques données binaires) qu'une zone mémoire de grande capacité (permettant de stocker un programme entier) au sein d'une mémoire vive ou d'une mémoire morte.

La mémoire vive 904 comporte notamment les registres suivants :

- un registre « *nb\_données* » dans lequel est conservée la longueur  $k$  de la séquence de données  $\underline{u}$ ,
- un registre «  $a$  », dans lequel est conservée la séquence  $\underline{a}$  obtenue en prolongeant  $\underline{u}$  au moyen de bits de bourrage,
- 5       - un registre «  $a^*$  » dans lequel est conservée la séquence entrelacée  $\underline{a}^*$ ,
- un registre «  $a,b,c$  » dans lesquels sont conservées les séquences  $\underline{a}$ ,  $\underline{b}$  et  $\underline{c}$  résultant du turbo codage, et
- un registre « *trame\_radio* » dans lequel est conservée l'intégralité de
- 10   la trame radio à émettre.

La mémoire morte 905 est adaptée à conserver, dans des registres qui, par commodité, possèdent les mêmes noms que les données qu'ils conservent :

- le programme de fonctionnement de l'unité centrale de traitement
- 15   900, dans un registre « *programme* »,
- les coefficients du polynôme  $g(x)$ , dans un registre «  $g$  »,
- les coefficients du polynôme  $f_1(x)$ , dans un registre «  $f_1$  »,
- les coefficients du polynôme  $f_2(x)$ , dans un registre «  $f_2$  »,
- la longueur des séquences  $\underline{a}$  et  $\underline{a}^*$ , dans un registre «  $p$  »,
- 20   - la permutation définissant l'entrelaceur (telle que l'équation (1) ci-dessus), dans un registre « *entrelaceur* », et
- la valeur  $N$  de la période de  $g$  dans un registre «  $N$  ».

La **figure 5** représente un dispositif de décodage 1101 apte à décoder des données fournies par un appareil tel que celui de la figure 4. Le

25   décodage après réception est effectué par un turbodécodeur constitué de deux décodeurs, de deux entrelaceurs  $\pi_1$ , d'un désentrelaceur  $\pi_2$ , d'un additionneur 70 et d'une unité de décision 80 ; les décodeurs, qui sont désignés par « Décodeur 1 » et « Décodeur 2 » sur la figure 5, peuvent être par exemple du type BCJR, c'est-à-dire utilisant l'algorithme de Bahl, Cocke, Jelinek et Raviv,

30   ou du type SOVA (en anglais : « *Soft Output Viterbi Algorithm* »).

Un turbodécodeur classique nécessite également un rebouclage de la sortie du désentrelaceur  $\pi_2$  sur l'entrée du premier décodeur afin de

transmettre au premier décodeur l'information dite « extrinsèque » produite par le second décodeur.

Le turbodécodeur 300 reçoit les séquences codées  $\underline{a'}$ ,  $\underline{b'}$  et  $\underline{c'}$  en provenance d'un récepteur 1106 (voir la figure 6). Une fois le décodage  
5 terminé, la séquence  $\underline{\hat{a}}$ , qui est une estimation de la séquence  $\underline{a}$  émise par l'émetteur 906, est envoyée à un module tronqueur 335 ; ce tronqueur 335, selon l'invention, produit une séquence  $\underline{\hat{u}}$  en ôtant les  $d$  derniers bits de  $\underline{\hat{a}}$  (correspondant aux bits de bourrage placé par le module 30 de la figure 2) ; enfin, cette séquence  $\underline{\hat{u}}$  est envoyée vers un destinataire d'informations 1110.

10 Le schéma synoptique de la **figure 6** représente un appareil de réception de signaux numériques 333 selon l'invention. Ce dernier comprend un clavier 1111, un écran 1109, un destinataire d'informations externe 1110, un récepteur hertzien 1106, conjointement reliés à des ports d'entrée/sortie 1103 d'un dispositif de décodage 1101 qui est réalisé ici sous la forme d'une unité  
15 logique.

Le dispositif de décodage 1101 comporte, reliés entre eux par un bus d'adresses et de données 1102 :

- une unité centrale de traitement 1100,
- une mémoire vive RAM 1104,
- 20 - une mémoire morte 1105, et
- lesdits ports d'entrée/sortie 1103.

Chacun des éléments illustrés en figure 6 est bien connu de l'homme du métier des micro-ordinateurs et des systèmes de transmission et, plus généralement, des systèmes de traitement de l'information. Ces éléments  
25 connus ne sont donc pas décrits ici. On observe, cependant, que :

- le destinataire d'informations 1110 pourrait être, par exemple, un périphérique d'interface, un afficheur, un modulateur, une mémoire externe ou un autre système de traitement de l'information (non représenté), et pourrait être adapté à recevoir des séquences de signaux représentatifs de parole, de  
30 messages de service ou de données multimédia notamment de type IP ou ATM, sous forme de séquences de données binaires,

- le récepteur hertzien 1106 est adapté à mettre en œuvre un protocole de transmission par paquets sur un canal non filaire, et à transmettre ces paquets sur un tel canal.

La mémoire vive 1104 conserve des données, des variables et des résultats intermédiaires de traitement, dans des registres de mémoire portant, dans la description, les mêmes noms que les données dont ils conservent les valeurs. La mémoire vive 1104 comporte notamment les registres suivants :

- des registres « *données\_reçues* », dans lesquels sont respectivement conservées les séquences reçues  $\underline{a'}$ ,  $\underline{b'}$ , et  $\underline{c'}$ ,
- 10 - des registres « *inf\_extrinsèques* », dans lesquels sont respectivement conservées les séquences intermédiaires de décodage en sortie du Décodeur 2 de la figure 5,
- un registre « *données\_estimées* », dans lequel sont conservées la séquence décodée  $\underline{\hat{a}}$  et la séquence entrelacée correspondante  $\underline{\hat{a}^*}$ ,
- 15 - un registre « *nb\_itérations* », dans lequel est conservée la valeur du nombre d'itérations déjà effectuées par le turbodécodeur,
- un registre « *nb\_données* » dans lequel est conservée la longueur de la séquence  $\underline{\hat{u}}$  issue du tronqueur 335, et
- un registre « *trame\_radio* » dans lequel est conservée l'intégralité de la trame radio reçue.
- 20

La mémoire morte 1105 est adaptée à conserver, dans des registres qui, par commodité, possèdent les mêmes noms que les données qu'ils conservent :

- le programme de fonctionnement de l'unité centrale de traitement 1100, dans un registre « *programme* »,
- 25 - les coefficients du polynôme  $g(x)$ , dans un registre « *g* »,
- les coefficients du polynôme  $f_1(x)$ , dans un registre « *f<sub>1</sub>* »,
- les coefficients du polynôme  $f_2(x)$ , dans un registre « *f<sub>2</sub>* »,
- la longueur des séquences  $\underline{\hat{a}}$  et  $\underline{\hat{a}^*}$ , dans un registre « *p* »,
- 30 - la permutation définissant l'entrelaceur, dans un registre « *entrelaceur* »,
- la valeur  $N$  de la période de  $g$  dans un registre « *N* », et

- le nombre maximal d'itérations dans un registre « *nb\_iteration\_max* ».

On notera que, dans certaines applications, il sera commode d'utiliser le même dispositif informatique (fonctionnant en mode multi-tâches) pour l'émission et la réception de signaux selon l'invention ; dans ce cas, les  
5 unités 901 et 332 seront physiquement identiques.

Les procédés selon l'invention peuvent être mis en œuvre au sein d'un réseau de télécommunications, comme le montre la **figure 7**. Le réseau représenté, qui peut par exemple être constitué par un des futurs réseaux de communication tels que les réseaux UMTS, est constitué d'une station dite  
10 « station de base » SB désignée par la référence 64, et de plusieurs stations « périphériques » SPi ( $i = 1, \dots, n$ , où  $n$  est un entier supérieur ou égal à 1), respectivement désignées par les références 66<sub>1</sub>, 66<sub>2</sub>, ..., 66<sub>n</sub>. Les stations périphériques 66<sub>1</sub>, 66<sub>2</sub>, ..., 66<sub>n</sub> sont éloignées de la station de base SB, reliées chacune par une liaison radio avec la station de base SB et susceptibles de se  
15 déplacer par rapport à cette dernière.

La station de base SB et chaque station périphérique SPi peuvent comprendre un dispositif de codage 901 tel que décrit en référence aux figures 4, 5 et 6, un bloc d'émission et un module radio muni d'un émetteur classique comportant un ou plusieurs modulateurs, des filtres et une antenne.

20 La station de base SB et chaque station périphérique SPi selon l'invention peuvent comprendre également un dispositif de décodage 1101 tel que décrit en référence aux figures 5 et 6, un bloc de réception et un module radio avec son antenne.

La station de base SB et les stations périphériques SPi peuvent  
25 comprendre de surcroît, selon les besoins, une caméra numérique, un ordinateur, une imprimante, un serveur, un télécopieur, un scanner ou un appareil photographique numérique.

Pour terminer, on présente ci-dessous les résultats d'une simulation de codage et de décodage selon l'invention. On a donc d'abord cherché à  
30 obtenir la valeur de  $e$  offrant au code associé la plus grande distance minimale possible, dans le cas, pouvant être utile en pratique, où

$$g(x) = 1 + x^2 + x^3, f_1(x) = 1 + x + x^3, f_2(x) = 1 + x + x^2 + x^3, \text{ et } p = 224 (M = 32).$$

TABLE 1

e	1	9	11	15	23	25	29	37	39	43	51	53
$w_2(e)$	14	38	22	22	38	38	22	30	38	22	30	22
$w_3(e)$	10	22	26	34	24	26	28	18	26	30	26	32
e	57	65	67	71	79	81	85	93	95	99	107	109
$w_2(e)$	38	14	22	38	22	22	22	22	14	22	22	30
$w_3(e)$	18	62	26	28	34	32	30	30	62	32	28	24
e	113	121	123	127	135	137	141	149	151	155	163	165
$w_2(e)$	22	38	30	14	38	38	30	22	38	30	22	30
$w_3(e)$	14	28	26	62	20	22	26	14	20	26	26	22
e	169	177	179	183	191	193	197	205	207	211	219	221
$w_2(e)$	38	22	30	38	14	14	30	30	22	30	30	22
$w_3(e)$	18	34	18	24	60	96	26	22	32	24	16	12

On désigne par  $w_r(e)$  le poids minimal pour l'ensemble des séquences codées  $\underline{v} = (\underline{a}, \underline{b}, \underline{c})$  associées aux séquences  $\underline{a}$  de poids  $r$  et telles que  $a(x)$  soit divisible par  $g(x)$ . On a calculé, pour chaque valeur « utile » de  $e$ , les valeurs de  $w_r(e)$  pour  $r = 2$  et pour  $r = 3$ . Ces résultats sont donnés dans la

# 5 Table 1.

On peut considérer que la valeur  $e = 71$ , pour laquelle  $w_2 = 38$  et  $w_3 = 28$ , est optimale.

On a alors simulé les performances de ce turbocode sur un canal à bruit blanc gaussien, pour cette valeur optimale de  $e$ . Les résultats ont été exprimés en termes de probabilité d'erreurs résiduelles, par trame « FER » (en anglais, « *Frame Error Ratio* ») d'une part, et par bit « BER » (en anglais, « *Bit Error Ratio* ») d'autre part, en fonction du rapport Signal sur Bruit « SNR » (en anglais, « *Signal to Noise Ratio* ») par bit d'information sur le canal. Ils sont représentés sur la figure 8.

Pour mettre en œuvre cette simulation, on a étudié plusieurs valeurs de SNR comprises entre 0,8 et 2,8 dB. Pour chacune de ces valeurs de SNR, on a engendré de façon aléatoire un certain nombre de séquences  $\underline{u}$ , et on a calculé, pour chacune de ces séquences, la séquence codée  $\underline{v} = (\underline{a}, \underline{b}, \underline{c})$  correspondante selon la présente invention. Sur chaque séquence « bruitée »  $(\underline{a}', \underline{b}', \underline{c}')$  qui en a résulté, on a effectué des itérations doubles de décodage, au nombre de 8 au moins et de 50 au plus. Après les 8 premières itérations, la simulation était interrompue dès que deux itérations (doubles) consécutives donnaient le même résultat.

Pour en déduire « expérimentalement » la valeur probable de la distance minimale du code, on a procédé de la manière suivante. Lorsque le décodage s'interrompait avant la 50<sup>ème</sup> itération, et lorsque la séquence « estimée »  $\hat{\underline{a}}$  n'était pas identique à la séquence  $\underline{a}$  dont elle était issue, on a calculé leur différence binaire, ou « séquence d'erreur »  $\underline{d} = \underline{a} + \hat{\underline{a}}$ ; puis on a calculé la séquence codée  $\underline{v} = (\underline{d}, \underline{b}(\underline{d}), \underline{c}(\underline{d}))$  correspondante selon la présente invention; enfin, on a calculé le poids binaire PB de cette séquence codée  $\underline{v}$ , et cette valeur de PB associée à une estimation erronée a été enregistrée. Cette procédure a été répétée avec autant de séquences  $\underline{u}$  qu'il s'avérait nécessaire

pour obtenir 25 séquences  $\hat{a}$  erronées pour chaque valeur étudiée du rapport Signal sur Bruit SNR.

Une fois la simulation achevée, on a constaté qu'aucune de ces séquences  $\underline{y}$  associées à une estimation erronée n'avait un poids  $PB$  inférieur à 5 28. Comme il est connu de l'homme du métier, ce résultat, combiné à la valeur relativement élevée de SNR atteinte (comme on peut le voir d'après la forme des graphiques illustrés sur la figure 8), est une forte indication que la distance minimale de ce turbocode doit être égale à 28.

## REVENDICATIONS

1. Procédé de turbocodage pour la transmission d'informations,  
 5 dans lequel, un premier polynôme à coefficients binaires  $g(x)$  de degré  $d$  et de terme constant égal à 1 ayant été prédéterminé, on présente d'abord lesdites informations sous la forme de séquences binaires  $\underline{u}$  de longueur

$$k = p - d,$$

où  $p$  est un multiple prédéterminé de la période  $N$  dudit polynôme  $g(x)$ , puis l'on  
 10 produit pour chacune desdites séquences  $\underline{u}$  un triplet  $\underline{v}$  de séquences binaires  $(\underline{a}, \underline{b}, \underline{c})$  destinées à être transmises et obtenues comme suit :

- ladite séquence  $\underline{a}$  est de longueur  $p$  et obtenue en prolongeant la séquence  $\underline{u}$  au moyen de  $d$  bits de « bourrage » de manière à ce que le polynôme

15 
$$a(x) = \sum_{i=0}^{p-1} a_i x^i$$

associé à  $\underline{a}$  soit divisible par  $g(x)$ ,

- ladite séquence  $\underline{b}$  est représentée par le polynôme

$$b(x) = a(x) \cdot f_1(x) / g(x),$$

où  $f_1(x)$  est un deuxième polynôme à coefficients binaires prédéterminé, sans  
 20 diviseur commun avec  $g(x)$ , et

- ladite séquence  $\underline{c}$  est représentée par le polynôme

$$c(x) = a^*(x) \cdot f_2(x) / g^*(x),$$

où

$$a^*(x) = \sum_{i=0}^{p-1} a_i x^{\pi(i)},$$

25 où  $\pi(i)$  est une permutation prédéterminée des entiers  $i$  compris entre 0 et  $(p-1)$ , où  $g^*(x)$  est un troisième polynôme à coefficients binaires prédéterminé, de degré  $d$  et de terme constant égal à 1,  $\pi(i)$  et  $g^*(x)$  étant choisis de manière à ce que, quel que soit le polynôme  $a(x)$  divisible par  $g(x)$  (mod. 2),  $a^*(x)$  soit divisible par  $g^*(x)$  (mod. 2), et où  $f_2(x)$  est un quatrième polynôme à coefficients  
 30 binaires prédéterminé, sans diviseur commun avec  $g^*(x)$ ,

caractérisé en ce que l'on prend pour  $\pi(i)$  le résidu modulo  $p$  du produit  $(i \cdot e)$ , où  $e$  est un nombre entier strictement positif prédéterminé, relativement premier avec  $p$ , congru à une puissance de 2 modulo  $N$ , et non congru à une puissance de 2 modulo  $p$ , d'où il résulte que  $g^*(x)$  est identique à  $g(x)$ .

5                    2. Procédé de turbodécodage, caractérisé en ce qu'il permet de décoder des séquences reçues qui ont été émises après avoir été codées à l'aide d'un procédé de turbocodage selon la revendication 1.

3. Procédé pour déterminer un procédé de turbocodage dans lequel, un premier polynôme à coefficients binaires  $g(x)$  de degré  $d$  et de terme  
10 constant égal à 1 ayant été prédéterminé, on présente d'abord lesdites informations sous la forme de séquences binaires  $\underline{u}$  de longueur

$$k = p - d,$$

où  $p$  est un multiple prédéterminé de la période  $N$  dudit polynôme  $g(x)$ , puis l'on produit pour chacune desdites séquences  $\underline{u}$  un triplet  $\underline{v}$  de séquences binaires  
15  $(\underline{a}, \underline{b}, \underline{c})$  destinées à être transmises et obtenues comme suit :

- ladite séquence  $\underline{a}$  est de longueur  $p$  et obtenue en prolongeant la séquence  $\underline{u}$  au moyen de  $d$  bits de « bourrage » de manière à ce que le polynôme

$$a(x) = \sum_{i=0}^{p-1} a_i x^i$$

20 associé à  $\underline{a}$  soit divisible par  $g(x)$ ,

- ladite séquence  $\underline{b}$  est représentée par le polynôme

$$b(x) = a(x) \cdot f_1(x) / g(x),$$

où  $f_1(x)$  est un deuxième polynôme à coefficients binaires prédéterminé, sans diviseur commun avec  $g(x)$ , et

25 - ladite séquence  $\underline{c}$  est représentée par le polynôme

$$c(x) = a^*(x) \cdot f_2(x) / g(x),$$

où

$$a^*(x) = \sum_{i=0}^{p-1} a_i x^{\pi(i)},$$

où  $f_2(x)$  est un troisième polynôme à coefficients binaires prédéterminé, sans diviseur commun avec  $g(x)$ , et où  $\pi(i)$  est le résidu modulo  $p$  du produit  $(i \cdot e^*)$ , où  $e^*$  est un nombre déterminé de la manière suivante :

a) on choisit un certain nombre de séquences  $\underline{u}$  différentes pour  
5 former ce que l'on appellera « l'ensemble représentatif »,

b) pour chaque nombre entier strictement positif  $e$  inférieur à  $p$ , congru à une puissance de 2 modulo  $N$  et relativement premier avec  $p$  :

- on calcule le poids binaire  $PB$  total de tous lesdits triplets de séquences binaires  $\underline{v}$  associés aux séquences  $\underline{u}$  appartenant audit ensemble  
10 représentatif, et

- on prend note de la valeur  $w(e)$ , associée à cette valeur de  $e$ , de la valeur minimale parmi tous ces poids binaires  $PB$ , et

c) on choisit, pour mettre en œuvre le codage, la valeur  $e^*$  de  $e$  qui est associée à la plus grande valeur de ce poids minimal  $w$ .

15 4. Dispositif de codage (901) de séquences de données destinées à être transmises à l'aide d'un procédé de turbocodage selon la revendication 1, caractérisé en ce qu'il comporte :

- des moyens (30) pour obtenir, pour chaque séquence de données  $\underline{u}$ , ladite séquence  $\underline{a}$  associée à  $\underline{u}$  en prolongeant la séquence  $\underline{u}$  au moyen  
20 desdits  $d$  bits de bourrage, et

- au moins un turbocodeur (40) comportant un entrelaceur  $\pi_1$  apte à réaliser la permutation prévue dans ledit procédé.

25 5. Dispositif de décodage (1101) destiné à mettre en œuvre un procédé de turbodécodage selon la revendication 2, caractérisé en ce qu'il comporte :

- au moins un turbodécodeur (300) comportant deux entrelaceurs  $\pi_1$  aptes à réaliser la permutation prévue dans ledit procédé, et un désentrelaceur  $\pi_2$  apte à inverser cette permutation, et

- des moyens (335) pour produire une séquence binaire  $\hat{\underline{u}}$  en ôtant  
30 les  $d$  derniers bits de la séquence estimée  $\hat{\underline{a}}$  obtenue à la fin du turbodécodage des séquences reçues  $\underline{a}'$ ,  $\underline{b}'$  et  $\underline{c}'$  correspondant respectivement auxdites séquences émises  $\underline{a}$ ,  $\underline{b}$ , et  $\underline{c}$ .

6. Appareil d'émission de signaux numériques codés (48), caractérisé en ce qu'il comporte un dispositif de codage selon la revendication 4, et en ce qu'il comporte des moyens (906) pour émettre lesdites séquences codées a, b, et c.

5                7. Appareil de réception de signaux numériques codés (333), caractérisé en ce qu'il comporte un dispositif de décodage selon la revendication 5, et en ce qu'il comporte des moyens (1106) pour recevoir lesdites séquences a', b', et c'.

10              8. Réseau de télécommunications, caractérisé en ce qu'il comporte au moins un appareil selon la revendication 6 ou la revendication 7.

9. Moyen de stockage de données lisible par un ordinateur ou un microprocesseur conservant des instructions d'un programme informatique, caractérisé en ce qu'il permet la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 3.

15              10. Moyen de stockage de données amovibles, partiellement ou totalement, lisible par un ordinateur et/ou un microprocesseur conservant des instructions d'un programme informatique, caractérisé en ce qu'il permet la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 3.

On désigne par  $w_r(e)$  le poids minimal pour l'ensemble des séquences codées  $\underline{v} = (\underline{a}, \underline{b}, \underline{c})$  associées aux séquences  $\underline{a}$  de poids  $r$  et telles que  $a(x)$  soit divisible par  $g(x)$ . On a calculé, pour chaque valeur « utile » de  $e$ , les valeurs de  $w_r(e)$  pour  $r = 2$  et pour  $r = 3$ . Ces résultats sont donnés dans la

# 5 Table 1.

On peut considérer que la valeur  $e = 71$ , pour laquelle  $w_2 = 38$  et  $w_3 = 28$ , est optimale.

On a alors simulé les performances de ce turbocode sur un canal à bruit blanc gaussien, pour cette valeur optimale de  $e$ . Les résultats ont été  
10 exprimés en termes de probabilité d'erreurs résiduelles, par trame « FER » (en anglais, « *Frame Error Ratio* ») d'une part, et par bit « BER » (en anglais, « *Bit Error Ratio* ») d'autre part, en fonction du rapport Signal sur Bruit « SNR » (en anglais, « *Signal to Noise Ratio* ») par bit d'information sur le canal. Ils sont représentés sur la figure 8.

15 Pour mettre en œuvre cette simulation, on a étudié plusieurs valeurs de SNR comprises entre 0,8 et 2,8 dB. Pour chacune de ces valeurs de SNR, on a engendré de façon aléatoire un certain nombre de séquences  $\underline{u}$ , et on a calculé, pour chacune de ces séquences, la séquence codée  $\underline{v} = (\underline{a}, \underline{b}, \underline{c})$  correspondante selon la présente invention. Sur chaque séquence « bruitée »  
20  $(\underline{a}', \underline{b}', \underline{c}')$  qui en a résulté, on a effectué des itérations doubles de décodage, au nombre de 8 au moins et de 50 au plus. Après les 8 premières itérations, la simulation était interrompue dès que deux itérations (doubles) consécutives donnaient le même résultat.

Pour en déduire « expérimentalement » la valeur probable de la  
25 distance minimale du code, on a procédé de la manière suivante. Lorsque le décodage s'interrompait avant la 50<sup>ème</sup> itération, et lorsque la séquence « estimée »  $\hat{\underline{a}}$  n'était pas identique à la séquence  $\underline{a}$  dont elle était issue, on a calculé leur différence binaire, ou « séquence d'erreur »  $\underline{d} = \underline{a} + \hat{\underline{a}}$  ; puis on a calculé la séquence codée  $\underline{v} = (\underline{d}, \underline{b}(\underline{d}), \underline{c}(\underline{d}))$  correspondante selon la présente  
30 invention ; enfin, on a calculé le poids binaire PB de cette séquence codée  $\underline{v}$ , et cette valeur de PB associée à une estimation erronée a été enregistrée. Cette procédure a été répétée avec autant de séquences  $\underline{u}$  qu'il s'avérait nécessaire.

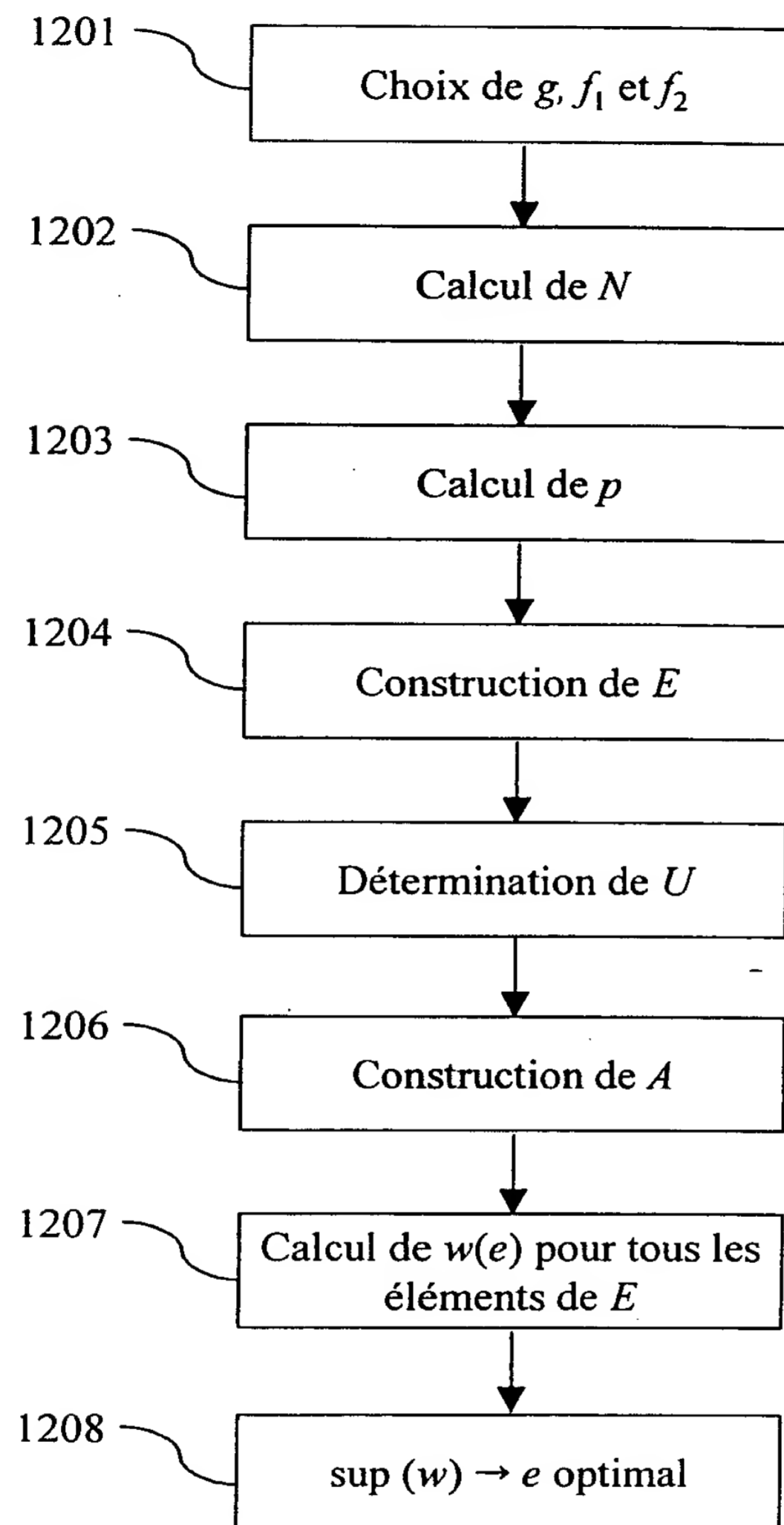


pour obtenir 25 séquences  $\hat{a}$  erronées pour chaque valeur étudiée du rapport Signal sur Bruit SNR.

Une fois la simulation achevée, on a constaté qu'aucune de ces séquences  $\underline{y}$  associées à une estimation erronée n'avait un poids  $PB$  inférieur à 5 28. Comme il est connu de l'homme du métier, ce résultat, combiné à la valeur relativement élevée de SNR atteinte (comme on peut le voir d'après la forme des graphiques illustrés sur la figure 8), est une forte indication que la distance minimale de ce turbocode doit être égale à 28.

TABLE 1

$e$	1	9	11	15	23	25	29	37	39	43	51	53
$w_2(e)$	14	38	22	22	38	38	22	30	38	22	30	22
$w_3(e)$	10	22	26	34	24	26	28	18	26	30	26	32
$e$	57	65	67	71	79	81	85	93	95	99	107	109
$w_2(e)$	38	14	22	38	22	22	22	22	14	22	22	30
$w_3(e)$	18	62	26	28	34	32	30	30	62	32	28	24
$e$	113	121	123	127	135	137	141	149	151	155	163	165
$w_2(e)$	22	38	30	14	38	38	30	22	38	30	22	30
$w_3(e)$	14	28	26	62	20	22	26	14	20	26	26	22
$e$	169	177	179	183	191	193	197	205	207	211	219	221
$w_2(e)$	38	22	30	38	14	14	30	30	22	30	30	22
$w_3(e)$	18	34	18	24	60	96	26	22	32	24	16	12

**FIG. 1**

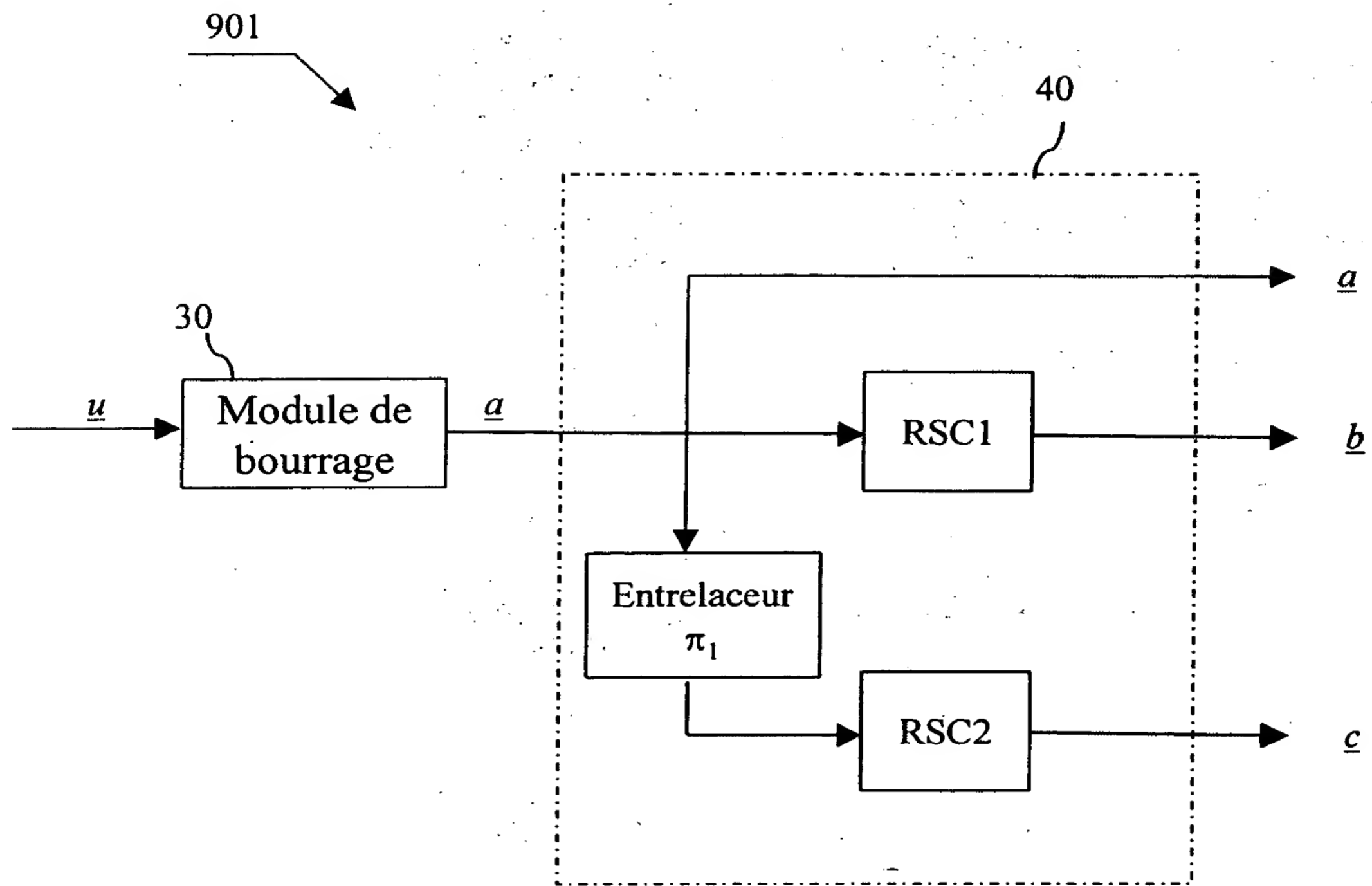


FIG. 2

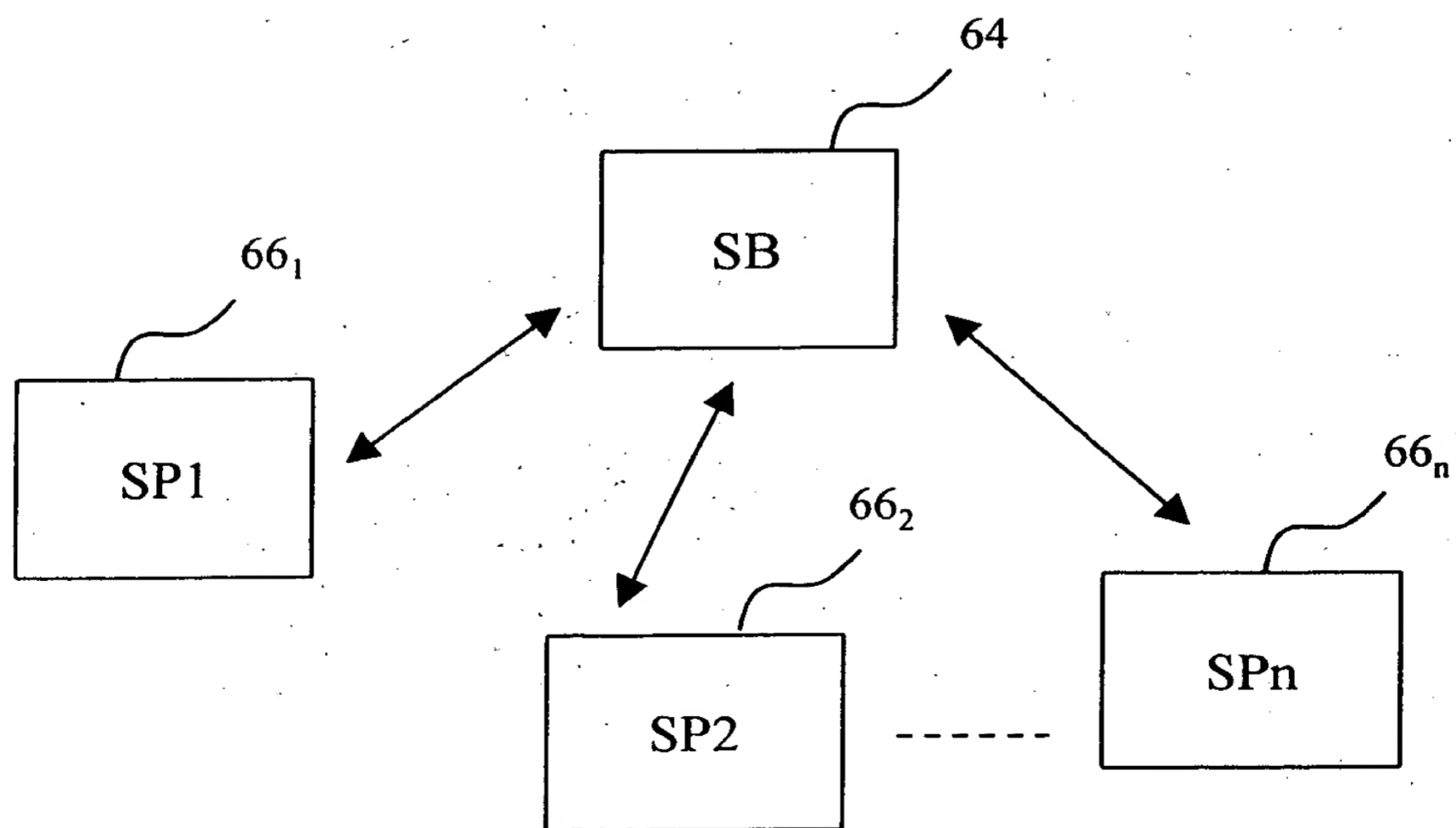


FIG. 7

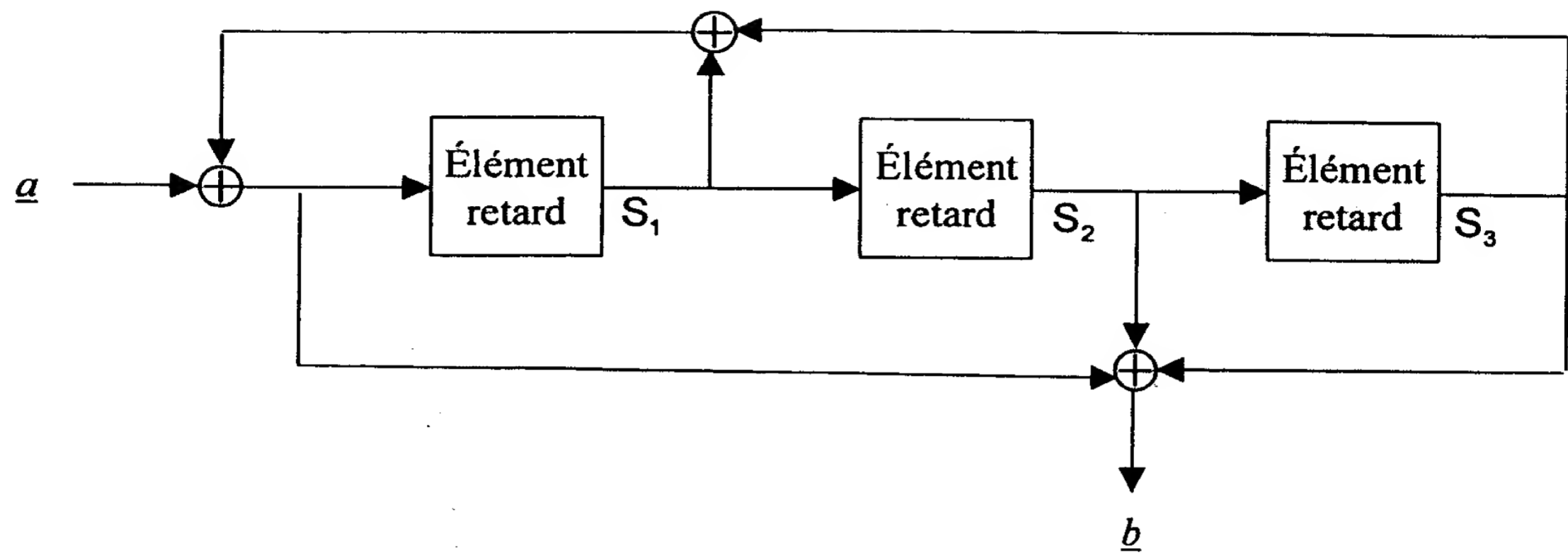


FIG. 3a

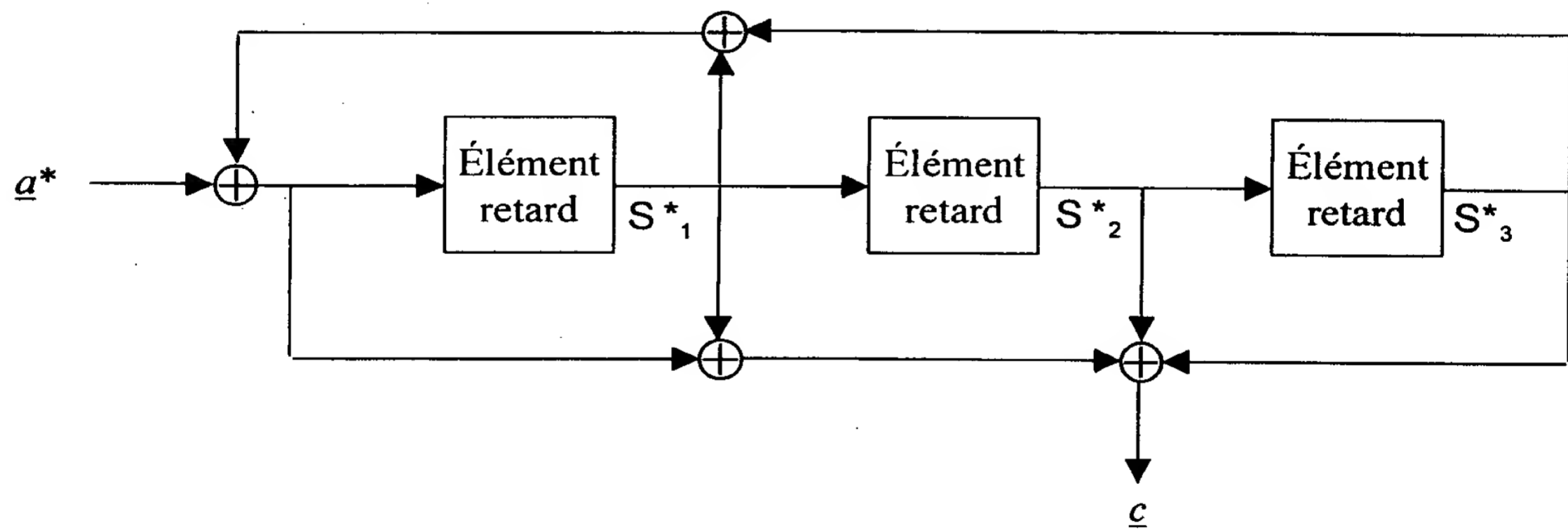


FIG. 3b

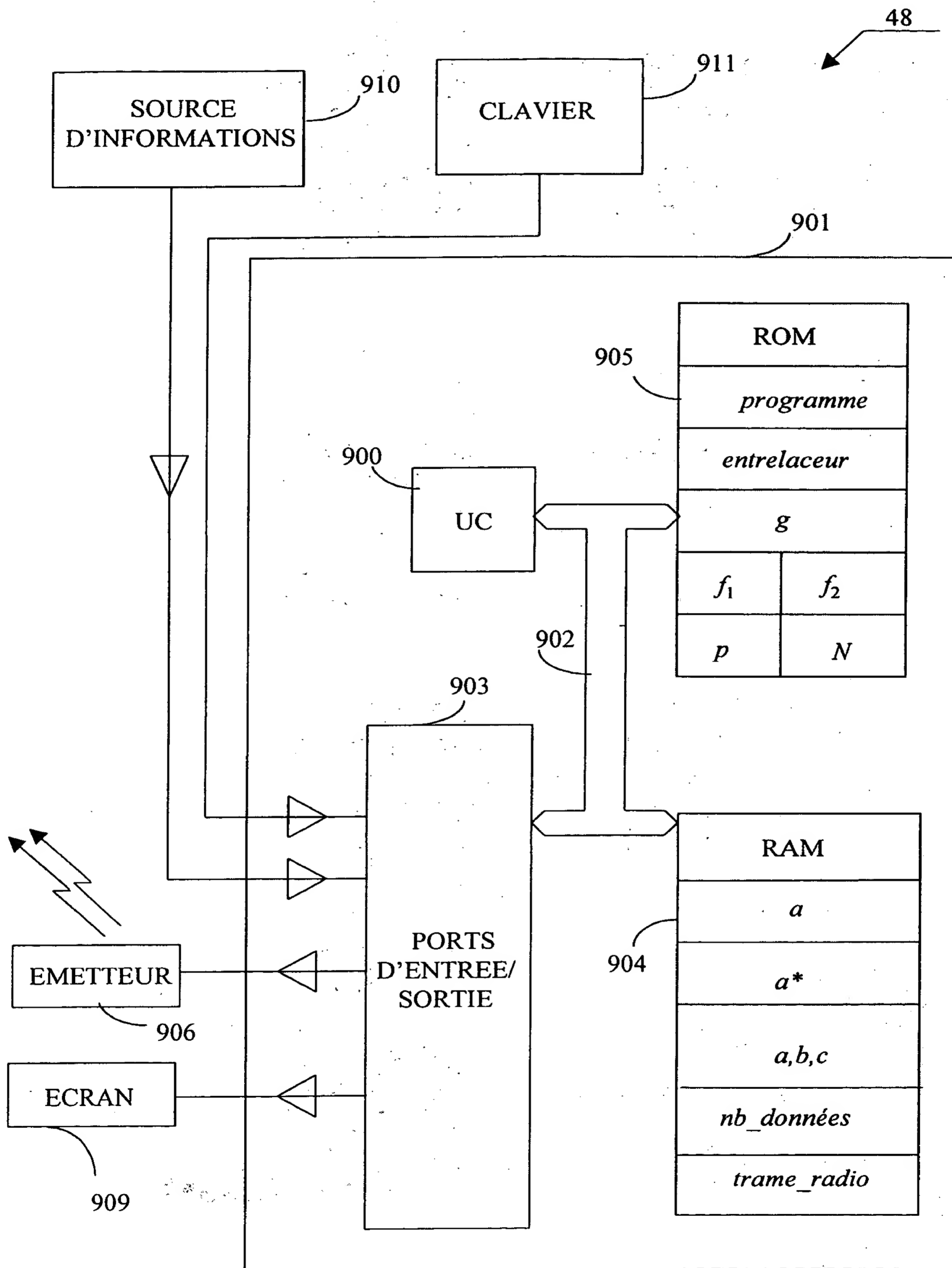


FIG. 4

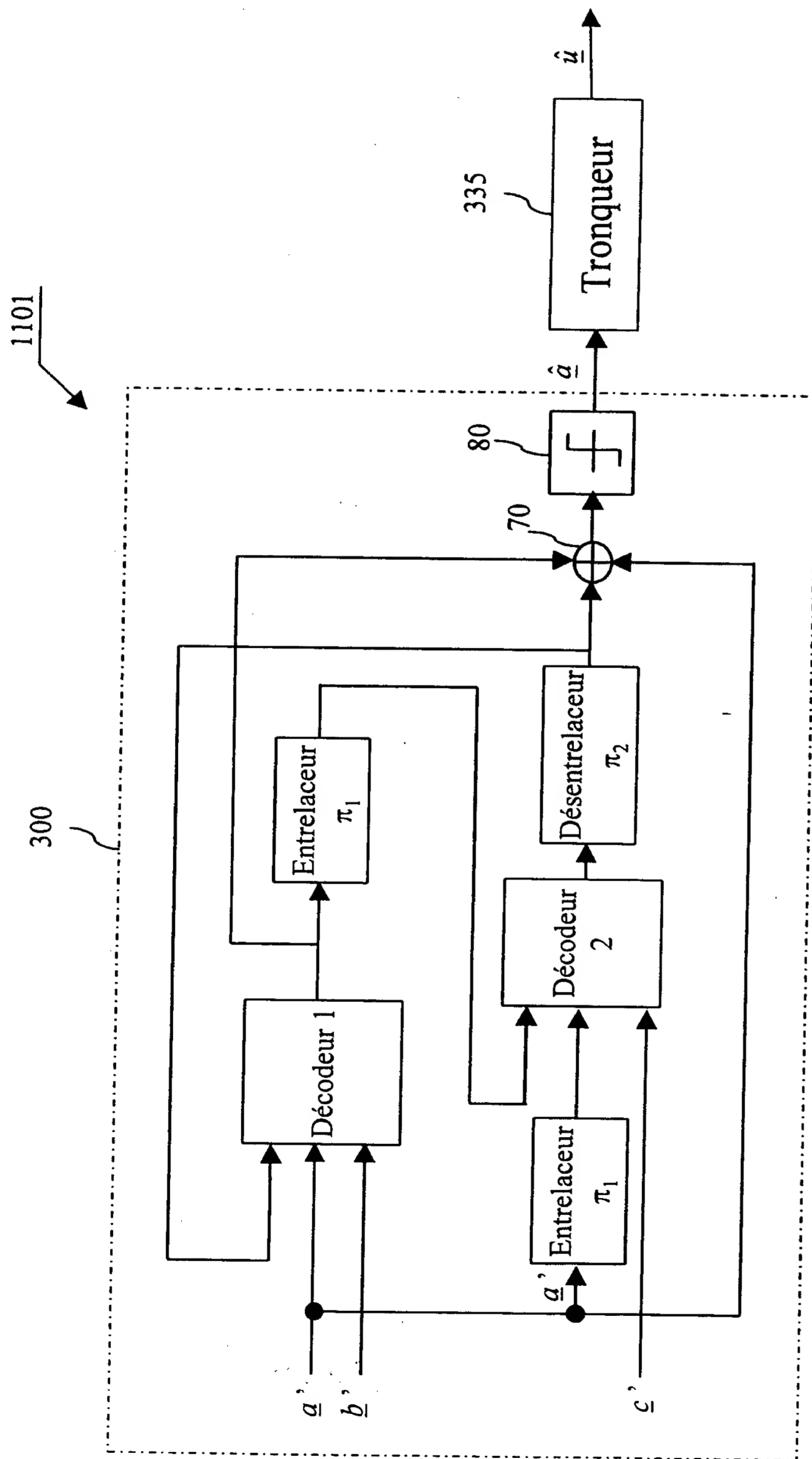


FIG. 5

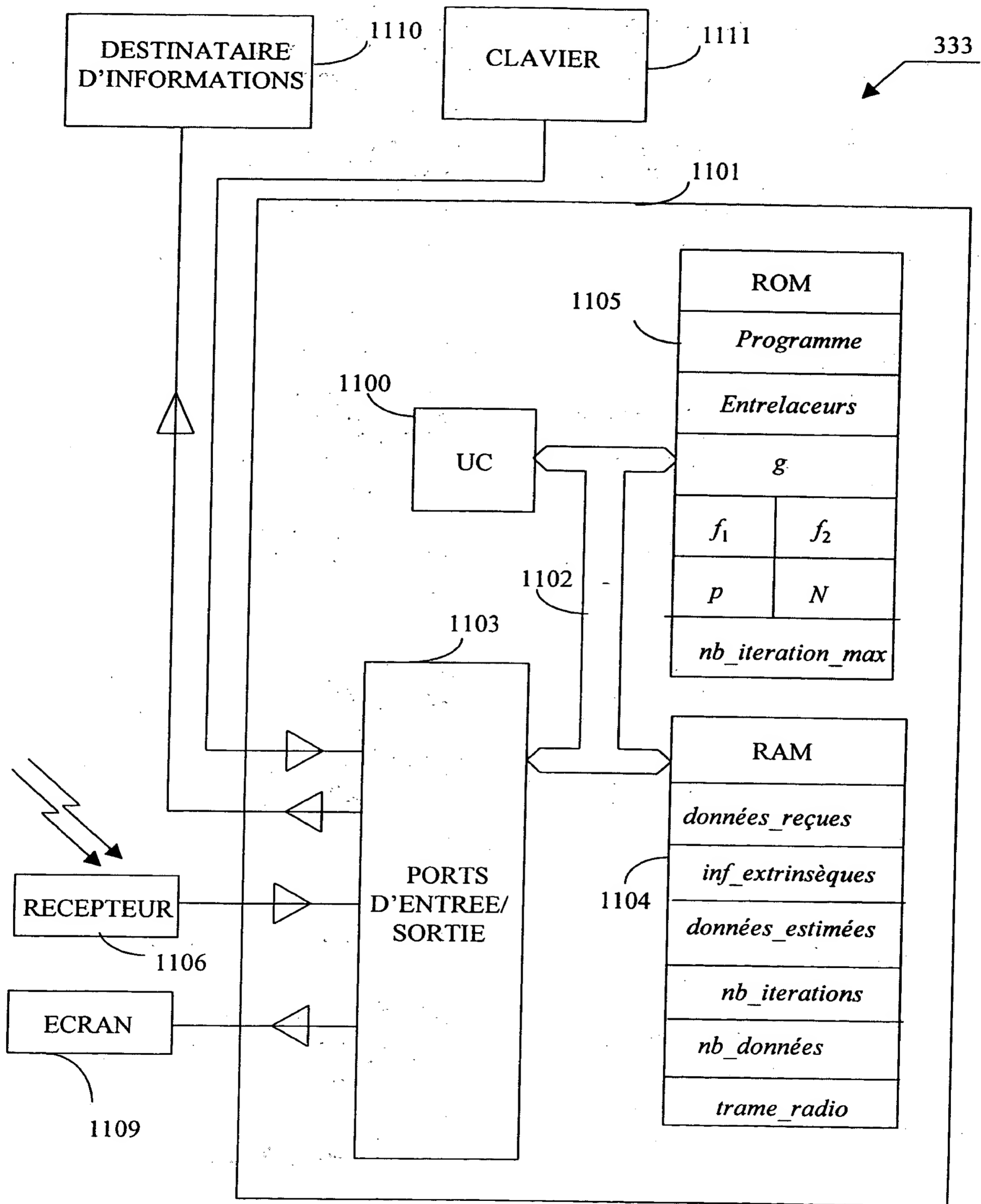
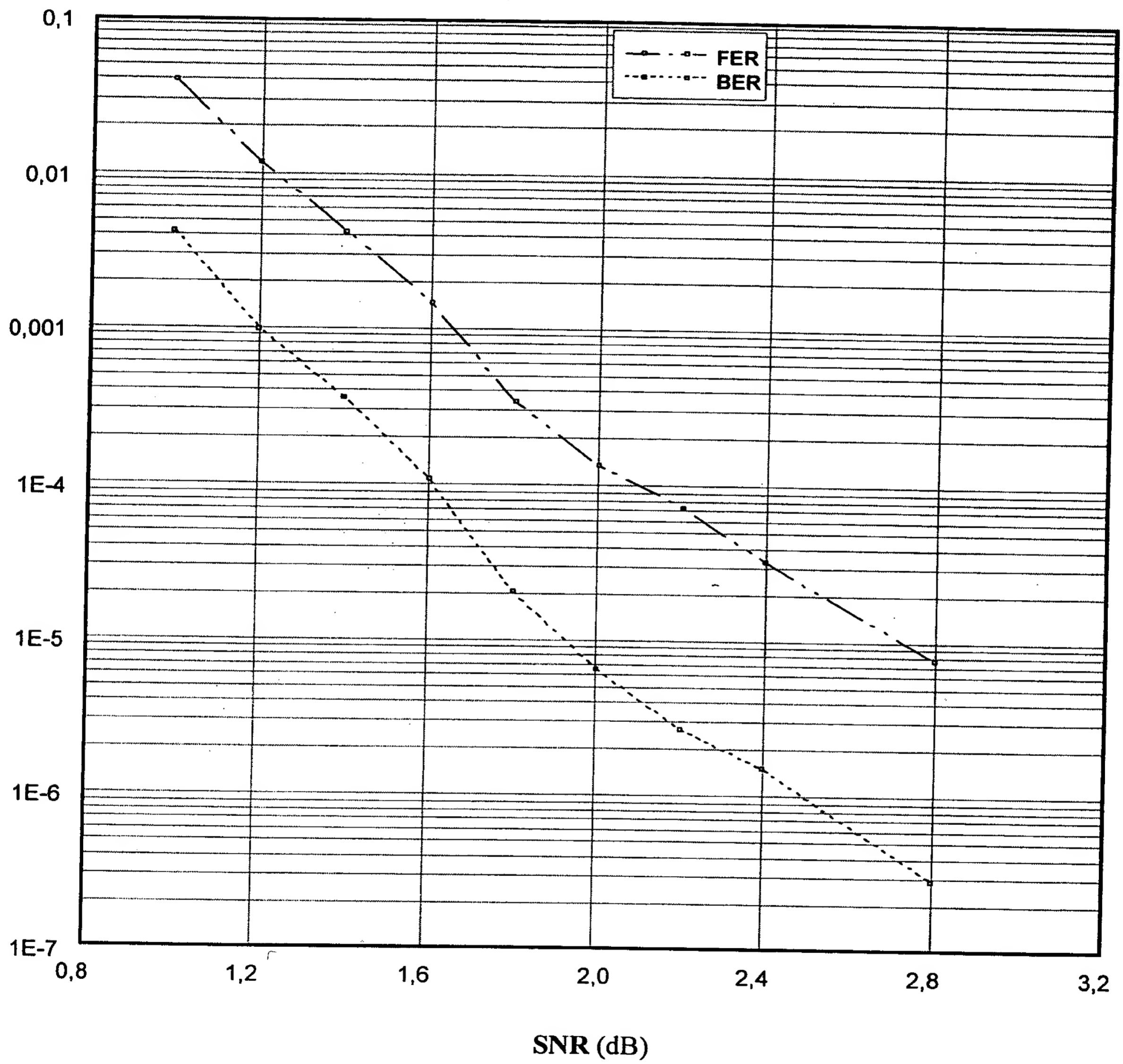


FIG. 6

**FIG. 8**